近日，腾讯安全联合实验室联合知道创宇发布《2018上半年区块链安全报告》（以下简称“《报告》”），梳理了2018年上半年围绕区块链爆发的典型安全事件，并给出防御措施，希望尽可能帮助用户避开区块链的“雷区”。

《报告》显示，截至目前，全球出现过的数字加密货币已超过1600种，这1600多种数字虚拟币中，存在大量空气币，被认为一文不值。但这1600多种数字虚拟币，在高峰时期，却撑起了6000亿美元的市值。排名前十位的加密数字货币，占总市场的90%，其中比特币、以太坊币分别占总市值的46.66%和20.12%。

加密数字货币一经诞生，安全性就是人们关注的焦点，遗憾的是各类重大安全事件层出不穷。

腾讯安全联合实验室和知道创宇公司认为：基于区块链加密数字货币引发的安全问题，来源于区块链自身机制安全、生态安全和使用者安全三个方面。上述三方面原因造成的经济损失分别是12.5亿美元、14.2亿美元和0.56亿美元。其中，区块链生态安全主要包括交易所被盗、交易所、矿池、网站被DDoS（分布式拒绝服务）、钱包、矿池面临DNS劫持风险、交易所被钓鱼、内鬼、钱包被盗、各种信息泄露、账号被盗等因素。

此外，区块链数字货币“热”背后也存在三大网络安全威胁：一方面，数字货币勒索事件频发，基础设施成勒索病毒攻击重点目标；另一方面，挖矿木马“异军突起”，成币圈价值“风向标”；此外，数字劫匪“铤而走险”攻击交易所，半年获利约7亿美元。

《报告》提出一些安全建议，对于区块链安全来讲，从系统架构上，建议相关企业与专业区块链安全研究组织合作，及时发现、修复系统漏洞，避免导致严重的大规模资金被盗事件发生。

对于普通网民而言，应防止电脑中毒成为被人控制的“矿工”，谨慎使用游戏外挂、破解软件、视频网站客户端破解工具，这些软件被人为植入恶意程序的概率较大。同时，安装正规杀毒软件并及时更新升级，当电脑卡顿、温度过热时，使用腾讯电脑管家进行检查，防止电脑被非法控制，造成不必要的损失。

对于企业网站、服务器资源的管理者，应部署企业级网络安全防护系统，防止企业服务器被入侵安装挖矿病毒，防止受到勒索病毒侵害。企业网站应防止被黑，及时修补服务器操作系统、应用系统的安全漏洞，避免企业服务器沦为黑客挖矿的工具，同时也避免因服务器被入侵而导致企业网站的访客电脑沦为“矿工”。